Attorney Docket: TN112

Claims 2, 3, 6, 7, 10 and 11 are rejected under U.S.C. §103(a) as being unpatentable over Nicolet and Devarakonda further in view of U.S. Patent No. 6,275,867 (Bendert et al.)(hereinafter "Bendert"). Claim 4 is rejected under U.S.C. §103(a) as being unpatentable over Nicolet and Devarakonda further in view of U.S. Patent No. 5,926,636 (Lam et al.)(hereinafter, "Lam"). Applicant respectfully traverses for the reasons set forth below.

Applicant's claimed invention is drawn to a system, method and server program embodied on a computer-readable medium for enabling a distributed network application that requires centralized administration via a master node to execute on the nodes of a clustered computing environment (where administration is not centralized). As set forth in detail in the subject specification, distributed network applications, such as that which might be written for BEA Systems Inc.'s Tuxedo® transaction manager and messaging middleware, often have defined the concept of a master machine that performs administration for the entire distributed application. (*Application No. 09/127,167*, p. 2) In the exemplary case of the Tuxedo environment, Logical Machines representing server machines are grouped together to define a domain. One of these Logical Machines is designated as the master, on which is running a DBBL process which performs administration for the entire Domain, including bringing a component online, taking a component offline, or checking the status of an individual component. (*Id.* at p.3).

A problem arises with such a distributed application when it is required to run in a clustered computing environment, such as by way of example, Microsoft Cluster Server (MSCS) in Microsoft® Windows NT®, Enterprise Edition, where administration is implemented on each of the connected systems (nodes) composing the cluster. As set forth in more detail in the specification, in the exemplary clustered environment, MSCS is controlled by the Cluster Service, which runs on each note of the cluster. (*Id.*). The Cluster Service spawns one or more Resource Monitors, each of which calls entry points in a Resource DLL, the latter of which implements the actions needed to bring the resource on-line or to take the resources off-line. (*Id.*). Thus, contrary to distributed network application that requires centralized administration via a master node, each node in the clustered computing environment maintains the administrative control.

Applicant's invention provides a solution to this problem. As set forth in claims 1, 4, 8, and 9, an administrative request from the clustered computing environment is first received at an originating node, and it is then determined whether the originating node is a designated master node for the distributed network application. If it is determined that the originating mode is not the designated master node, then

Serial No. 09/127,167   2

Attorney Docket: TN112

the administrative request is routed to that node which is the designated master node. (*See, Serial No. 09/127,167, claims 1, 4, 8 and 9*).

Nicolet discloses a method for providing secure management of remote servers. The invention set forth therein strives to achieve a balance between security and simplicity in the development of applications for network operating systems where remote computers are communicating with each other. According to Nicolet, in current such network operating systems, the application developer either has too much access/information about the network operating systems (i.e., in a remote console approach which relies on the user of the client to know how to interact with the remote computer), thus resulting in a lack of robust security, or else it is required that the developer do too much – e.g., implement the protocol and write the client and server applications address the problem of security in the software development of applications - again requiring that the developer have access to the system internals of one or more of the remote operating systems in order to effect the implementation with reduced security. (*Id.* at Col. 2, lines 15-62). According to Nicolet, this problem is resolved via the implementation of a set of secure remote procedure calls in an NCP network environment using the terms of native communications protocol of the local and remote computers. These remote procedure calls allow client software to directly interact with the operating system of the remote computers. (*Nicolet,* Col. 3, lines 49-62). In one embodiment, the remote procedure calls that have been implemented include mounting and dismounting remote volumes (*Id.*, Col. 3, lines 4-10).

The Examiner states that Nicolet teaches "*intercepting an administrative request (remote procedure calls) and routing the administrative request to the designated master node (server operating system).* (*Office Action dated May 23, 2002,* p. 2). Applicant respectfully disagrees with the Examiner's characterization of the server operating system as a "master node." As set forth in Applicant's application, a master node is system that controls the various administrative actions for the all the nodes in the network; in the case of Tuxedo®, all of the Logical Machines in the Domain. The server operating system to which Nicolet alludes is not equivalent to a master node as set forth in Applicant's application. Furthermore, from the foregoing it can be seen that Nicolet does not address the problem of enabling a distributed application requiring centralized control via a master node to execute on the nodes of a clustered computing environment (where administration is not centralized), and does not set forth receiving an administrative request from the clustered computing environment at an originating node, determining whether the originating node is a designated master node for the distributed network application, and then routing the request to the master node if it is determined that the originating mode is not the designated master node.

Serial No. 09/127,167   3

Attorney Docket: TN112

Applicant agrees with the Examiner that Nicolet does not teach determining if the originating node is the designated master node and is capable of processing the request. However, Examiner states that Devarakonda teaches that a node can process a request based on affinity information, which in turn could be based on the fact that a client may have an affinity with a node of the cluster. Devarakonda seeks to increase the processing capability of Web-based sites through the use of an encapsulated affinity-based router and method for such routing. In the environment envisioned in Devarakonda, a computer network includes encapsulated cluster of nodes (which appear as one node to the client, and thus "transparent"), and the router and routing method of the invention routes requests based on the application's affinity to nodes based on the state of the server (Devarakonda, para. [0017] and [0018]). Such affinity could be set statically, based on previous routing decisions or server state information, or logical proximity to the portion of the application in question (e.g., a portion of a portioned database is running on the node in question). (Id., [0038]) Applicant respectfully disagrees that Devarakonda teaches or suggests that such affinity could be based on the designation of the node as a master node. However, even if such affinity could be so based, Devarakonda does teach or suggest by itself, or in combination with Nicolet, Applicant's invention of enabling a distributed network application that requires centralized administration via a master node to execute on the nodes of a clustered computing environment, by receiving an administrative request from the clustered computing environment at an originating node, determining whether the originating node is a designated master node for the distributed network application, and then routing the request to the master node if it is determined that the originating mode is not the designated master node.

Claims 2, 3, 6, 7, 10, and 11 are rejected under Nicolet and Devarakonda further in view of Bendert. The Examiner states that Bendert teaches facilitating communication in a distributed processing system through the use of named pipes. However, Bendert does not teach or suggest either alone, or in combination with Nicolet and Devarakonda, Applicant's invention of enabling a distributed network application that requires centralized administration via a master node to execute on the nodes of a clustered computing environment, by receiving an administrative request from the clustered computing environment at an originating node, determining whether the originating node is a designated master node for the distributed network application, and then routing the request to the master node if it is determined that the originating mode is not the designated master node.

Claim 4 is rejected under Nicolet and Devarakonda further in view of Lam. The Examiner states that Lam teaches calling an administrative application programming interface (API). However, Lam does not teach or suggest either alone, or in combination with Nicolet and Devarakonda, Applicant's invention

Attorney Docket: TN112

of enabling a distributed network application that requires centralized administration via a master node to execute on the nodes of a clustered computing environment, by receiving an administrative request from the clustered computing environment at an originating node, determining whether the originating node is a designated master node for the distributed network application, and then routing the request to the master node if it is determined that the originating mode is not the designated master node.
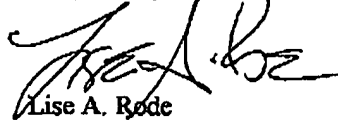
Thus, for the foregoing reasons, Applicant respectfully submits that independent claims 1, 5, and 8, and dependent claim 9 are patentable under 35 U.S.C. §103(a) over Nicolet in view of Devarakonda. Furthermore, claims 2, 3, 6, 7, 10 and 11 are patentable under 35 U.S.C. §103(a) over Nicolet and Devarakonda in view of Bendert. Finally, Applicant also respectfully submits claim 4 is patentable under 35 U.S.C. §103(a) over Nicolet and Devarakonda in view of Lam. Reconsideration of these claims and the application as a whole is thus respectfully solicited.

It is believed that all of the stated grounds of rejection have been properly traversed, accommodated, or rendered moot. It is further believed that a full and complete response has been made to the outstanding Office Action, and as such, the present application, including claims 1-11, is in condition for allowance. Applicants therefore respectfully request prompt and favorable consideration of

Serial No. 09/127,167   5

Attorney Docket: TN112

this amendment. If the Examiner believes that personal communication will expedite prosecution of this application, the Examiner is invited to telephone the undersigned at (215) 986-5169.
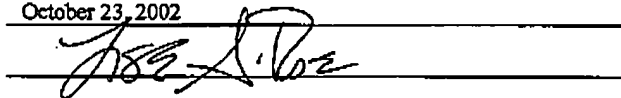
Respectfully submitted,

Lise A. Rode
Attorney for Applicant
Reg. No. 37,226

Unisys Corporation
Unisys Way, M/S E8-114
Blue Bell, Pennsylvania 19424-0001

The Director for Patents is hereby authorized to charge payment to Deposit Account No. 19-3790 of any fees associated with this communication.

I hereby certify that this correspondence is being transmitted via facsimile ((703) 305-3431) to the United States Patent and Trademark Office on the date shown below.

October 23, 2002

Serial No. 09/127,167   6

VERSION WITH MARKINGS TO SHOW CHANGES MADE

4.   The method recited in claim [1]2, further comprising the steps of:

receiving the administrative request at the master node via the named pipe; and

calling an administrative application programming interface (API) of the distributed network application to initiate processing of the request by the designated master node.